InfoBrief, sponsored by Akamai
JANUARY 2024

Next-Generation Trusted Public Services

How European Governments Can Boost Cyber-Resilience Through Modern Intelligent Security Architectures

Massimiliano Claps
Research Director

Remi Letemple
Senior Research Analyst,
IDC Government Insights

Romain Fouchereau
Research Manager,
European Security

Executive Summary

To deliver next-generation public services, European governments must invest in emerging technologies, enhance cyber-resilience, and build trust. This strategic approach aims to achieve practical outcomes:

Improving citizen experience:

- Governments are adopting modern security measures to provide citizens with secure and seamless interactions when accessing public services, aiming to build trust and reliability.

Increasing operational efficiency and resilience:

- Advanced security measures are being integrated to improve operational efficiency and build resilience against evolving threats, ensuring continuous service delivery and protecting critical operations.

Enhancing employee productivity:

- Modernising security architectures is a strategic move to empower government employees with secure and efficient workflows, boosting overall productivity.

Driving innovation through investment in emerging technologies:

- Proactive investments in emerging technologies aim to accelerate technology-enabled innovation, positioning governments at the forefront of cutting-edge solutions.

But transformation comes with challenges:

Expanding attack surface and broadening threat types:

- Digital transformation increases the attack surface, necessitating governments to fortify security measures and address a broader range of sophisticated cyberthreats.

Navigating regulations and compliance:

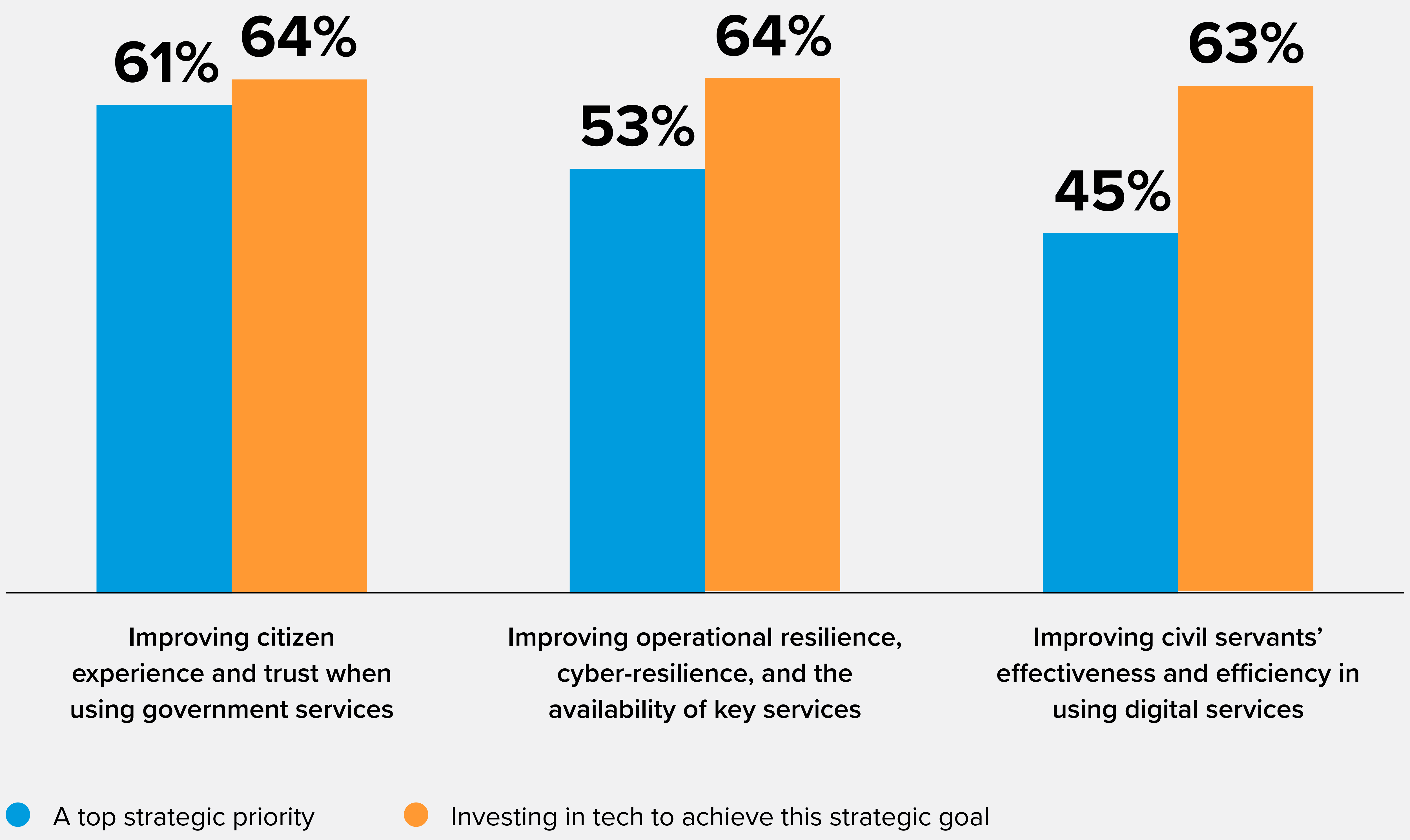
- Adherence to regulations and compliance standards is critical. Governments are navigating this landscape carefully to ensure the secure and lawful deployment of technologies in public services.

Modernising legacy systems with key focus areas:

- Modernisation efforts include advances in cloud security, network security, and zero trust frameworks. These technologies come together to enhance security and elevate citizen experience.

European senior government leaders have set clear priorities

Top 3 Strategic Priorities



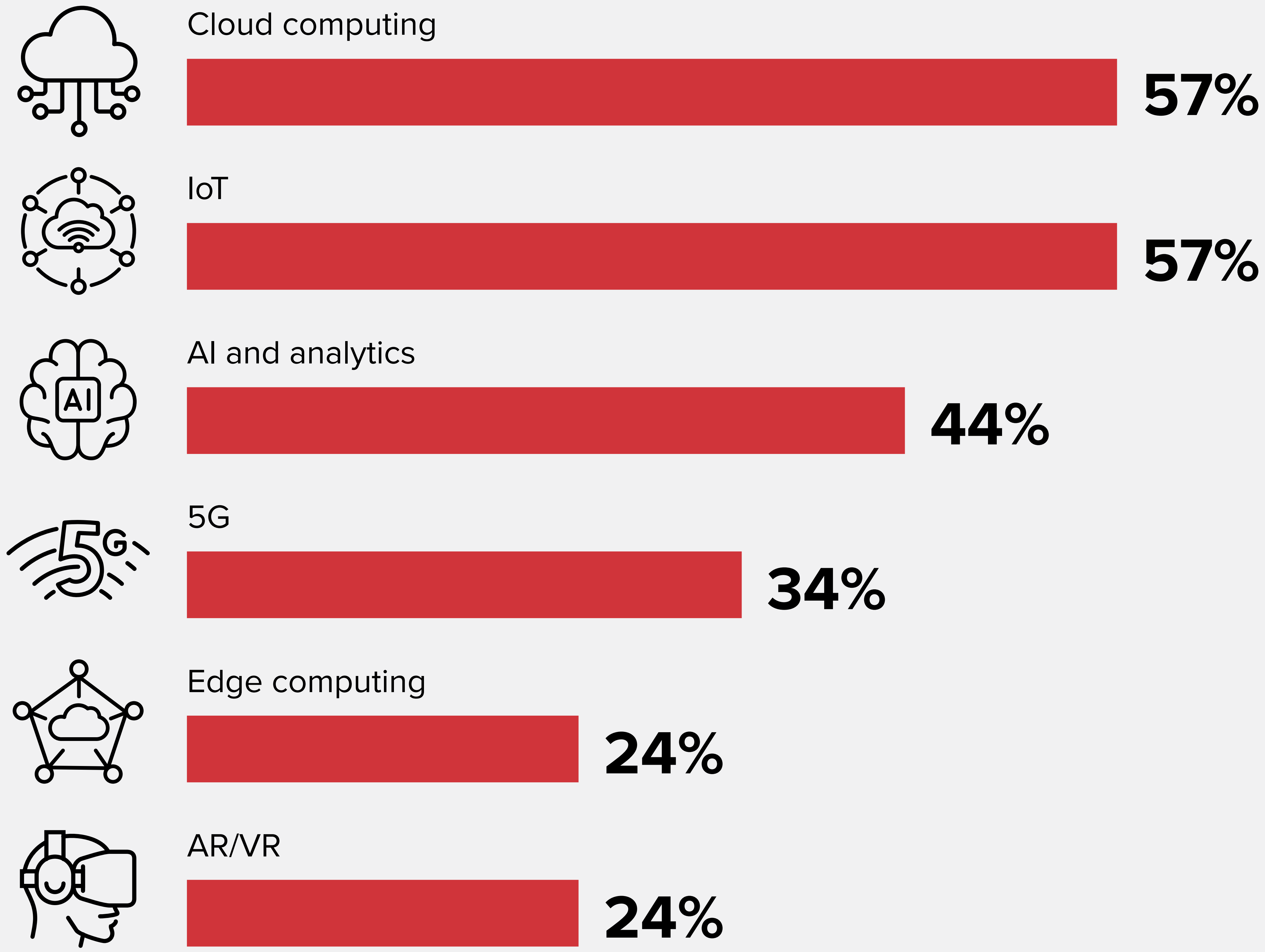
Accelerated by global dynamics and economic shifts, European senior civil servants are embracing technological innovation to shape the next generation of public services, aligning with citizen expectations and strategic funding for green and digital transitions.

Government executives aim to use technology to deliver **trusted customer experiences** and to use data and automation in an intelligent manner to **increase operational resilience and civil servants' productivity**.

Source: IDC's *Government Survey*, conducted for Akamai, August/September 2023 (N = 100); top 2 boxes on a 5-point scale

European governments are investing in emerging technologies to accelerate technology-enabled innovation

Extensions of Existing Solutions Governments Plan to Implement



European civil servants recognise the imperative of establishing a robust foundation for the successful adoption of emerging technologies.

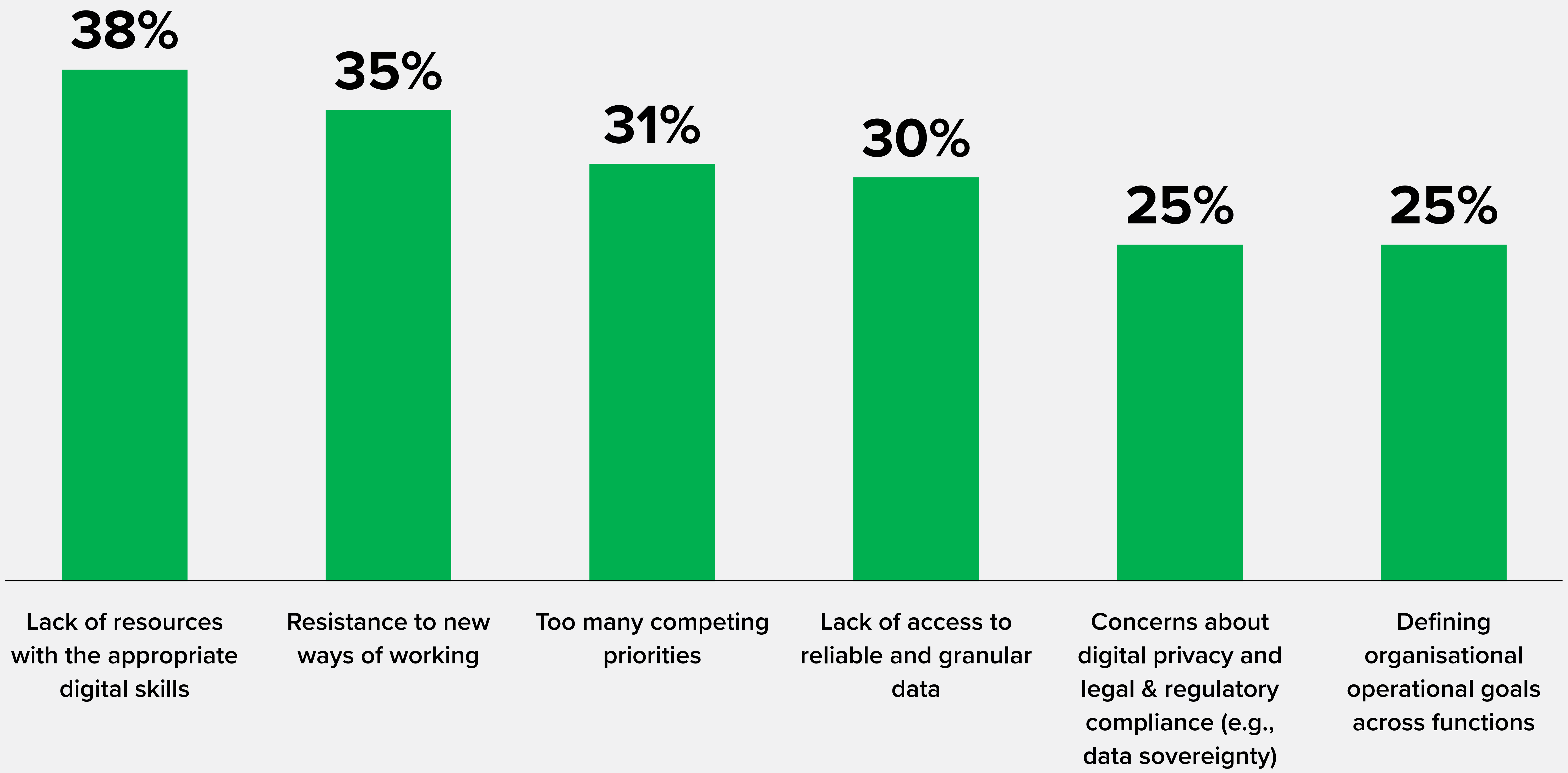
This foundation should consist of **integrated cloud-centric infrastructure and platforms — a seamless connectivity framework incorporating IoT, edge, and mobile devices**.

This approach will enable European governments to harness the full potential of emerging technologies, providing a **comprehensive and interconnected ecosystem** for driving technological **advances in public services**.

Source: IDC's *Government Survey,* conducted for Akamai, August/September 2023 (N = 100)

Senior government leaders in Europe understand that technology is not the only barrier to delivering next-generation public services

Key Innovation Challenges



As well as selecting and deploying the right technologies, European governments need to tackle organisational challenges, lack of access to reliable data, and regulatory compliance concerns to achieve their strategic goals.

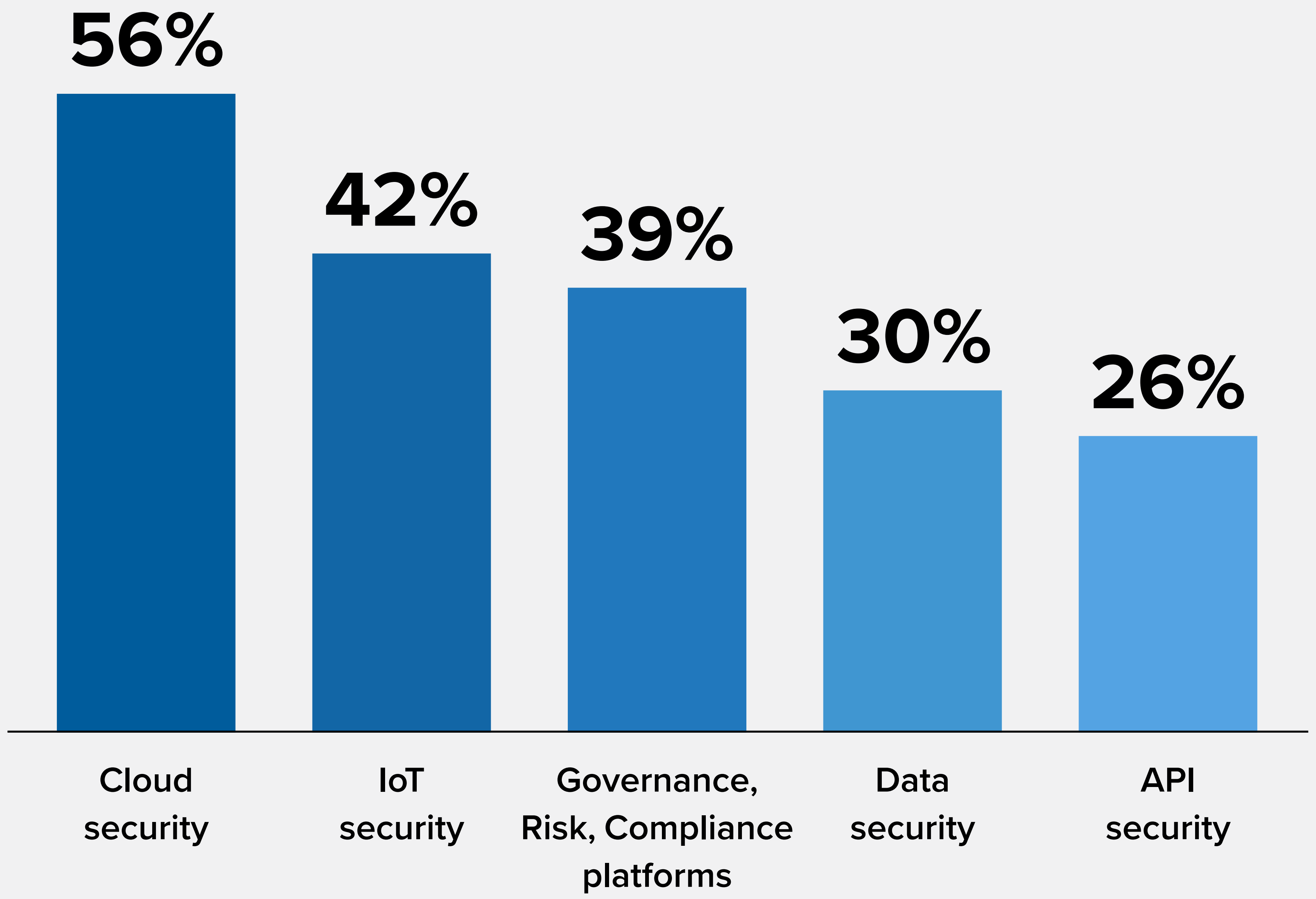
By engaging with the right partners, governments will acquire cutting-edge technologies and remove the operational burden associated with implementation. This approach addresses technological needs and tackles resistance to change by **providing guidance and seamless integration**.

Source: IDC's *Government Survey,* conducted for Akamai, August/September 2023 (N = 100)

Cloud security will boost resilience

As organisations embrace cloud, strategic partnerships emerge that can address multiple challenges. By aligning with the right partners, organisations can seamlessly migrate to the cloud, ensure the protection of sensitive data, secure cloud-native applications, and address the challenges associated with cloud adoption. They can also leverage the full scalability and agility that cloud environments offer.

Top 5 IT Security Technology Priorities



Benefits

- **Scalability:** Cloud environments provide the scalability necessary to meet the demands of modern government services.
- **Cost Efficiency:** Efficient cloud resource management reduces operational costs, maximising taxpayer value.
- **Agility:** Quick and flexible access to resources accelerates innovation and improves service delivery.
- **Resilience:** Redundancy and disaster recovery options in the cloud enhance business continuity and resilience.
- **Collaboration:** Cloud services facilitate inter-agency collaboration, improving efficiency and public service quality.

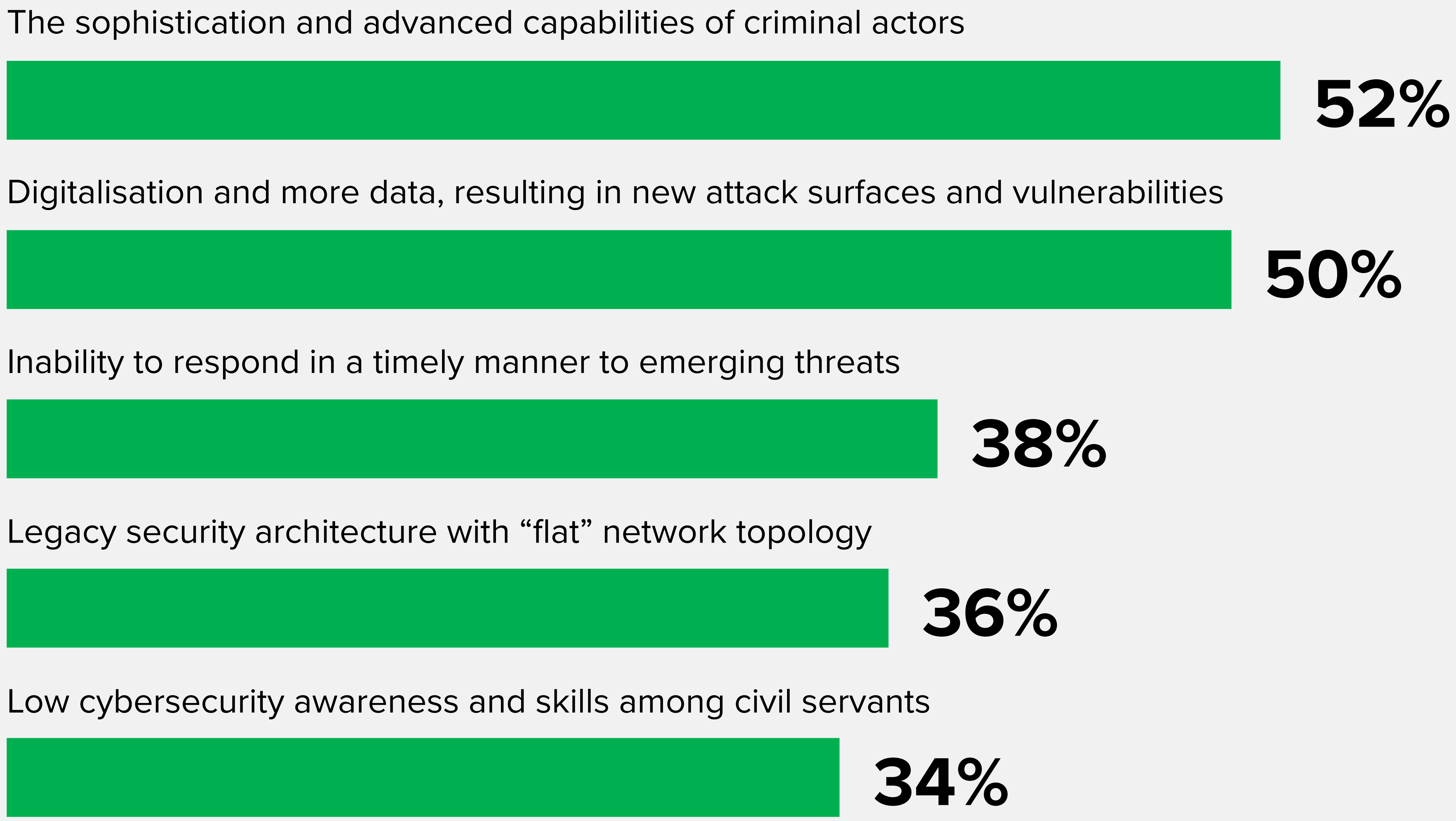
Challenges

- **Data Protection:** Cloud adoption expands the attack surface for sensitive data. Robust encryption and access controls are essential to ensure data remains confidential and compliant with regulations.
- **Identity and Access Management:** Managing identities and access across cloud services is complex. Secure identity management is crucial to prevent unauthorised access.
- **Securing Cloud-Native Applications:** Cloud-native applications require specific security measures, including robust API and container security, to protect against modern cyberthreats.
- **Compliance Challenges:** Maintaining compliance with data protection regulations, even in a cloud environment, is a critical concern.

Source: IDC's *Government Survey,* conducted for Akamai, August/September 2023 (N = 100)

Further digitalising government services and processes increases cyber-vulnerabilities in the public sector

Major Challenges in Responding to Cyberthreats



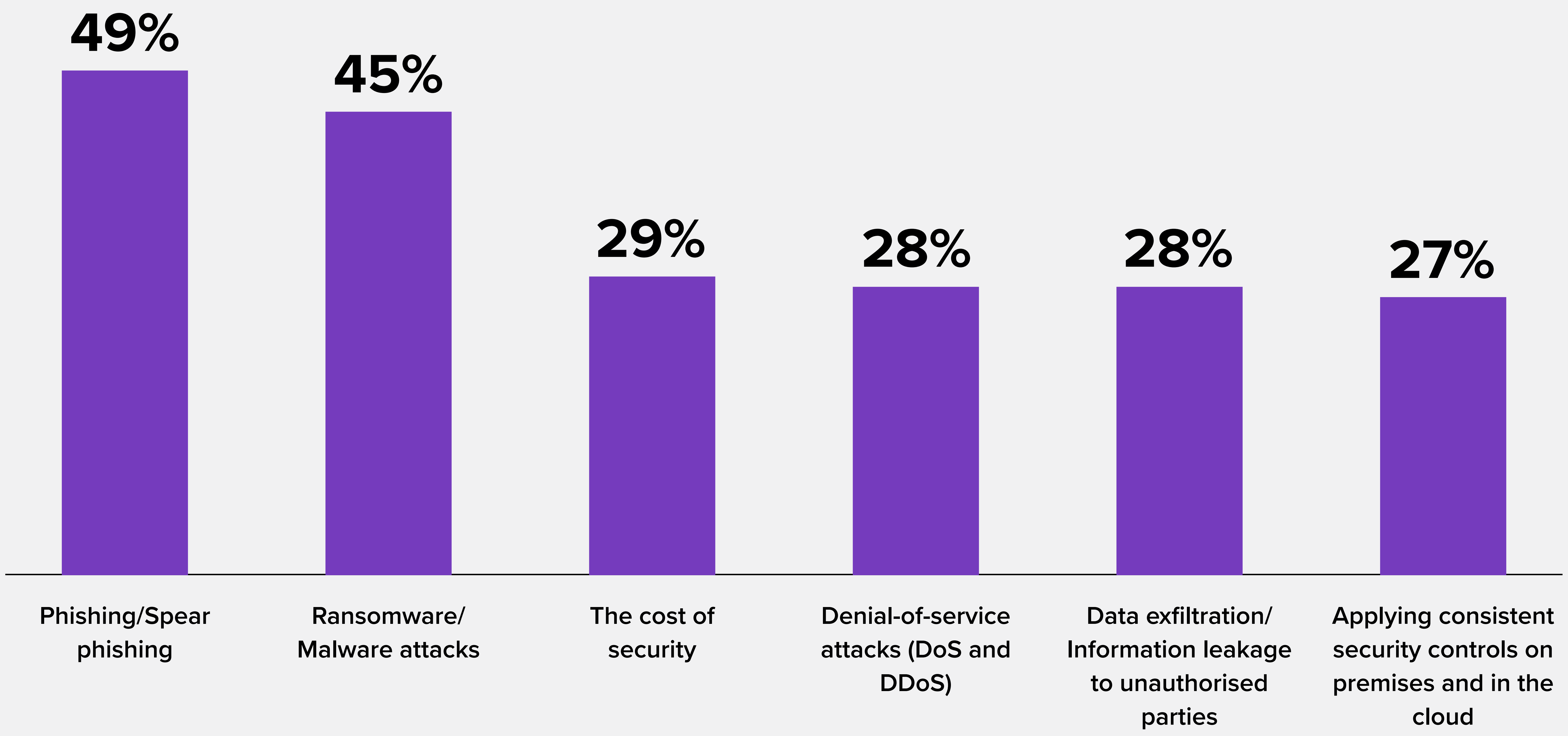
To realise the value of technology innovation, European governments must also tackle its risks, starting with **cybersecurity**.

The expanding availability of services and data online, inadequate operational and architectural capabilities and capacity, and limited awareness and skills, combined with civil servants not applying good cybersecurity practices, all increase the public sector’s exposure to cyberattacks, which are growing in volume and sophistication.

Source: IDC’s *Government Survey,* conducted for Akamai, August/September 2023 (N = 100)

Cybercriminals rapidly adopt new technologies as they emerge to increase the speed and sophistication of their attacks

Most Common Security Challenges Encountered in the Past Year

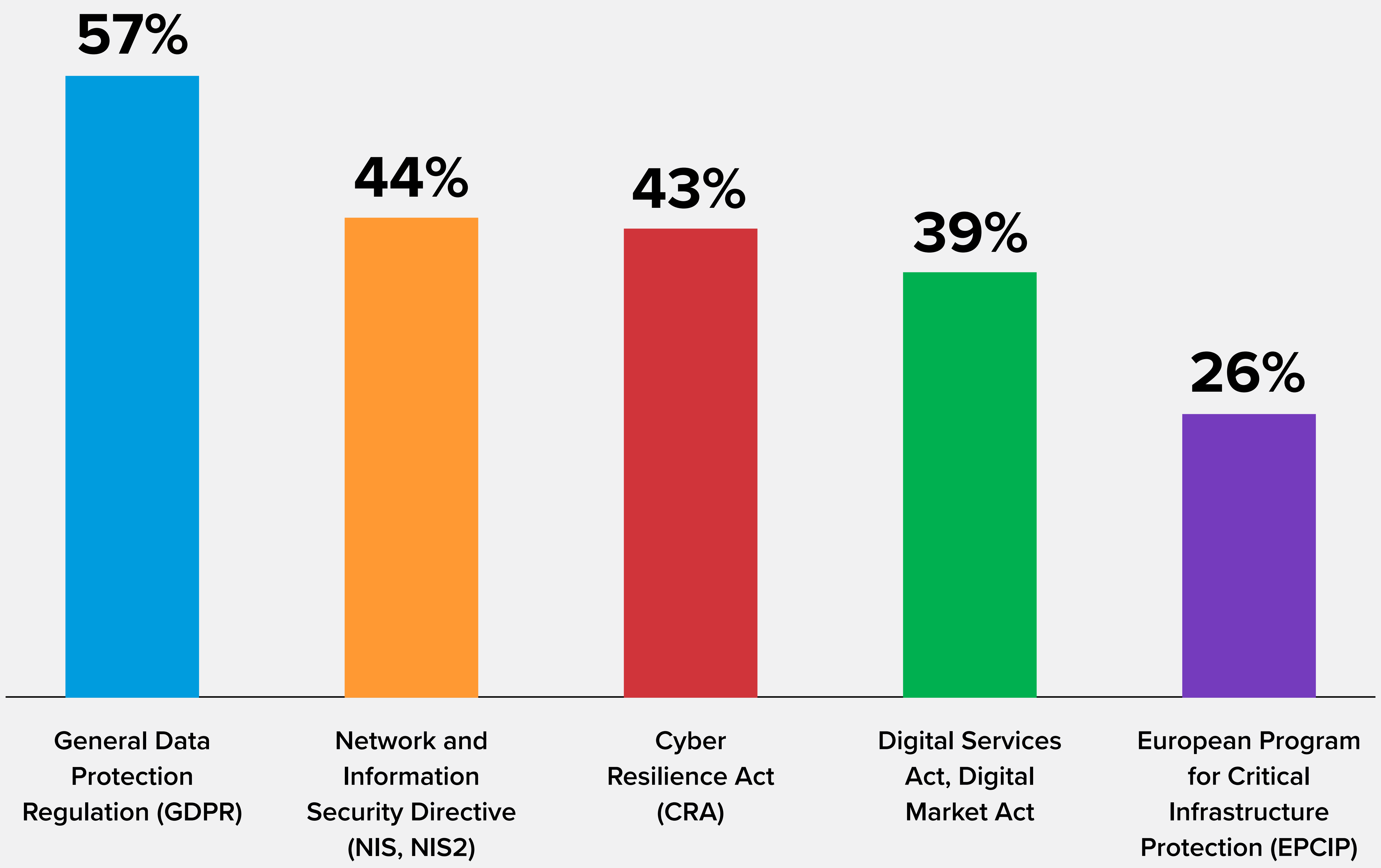


The same emerging technologies that allow governments to improve their services are empowering **cybercriminals** to increase the **sophistication** and scale of phishing, ransomware, and DDoS attacks, such as by leveraging malicious bots to replicate the look and feel of government websites and conduct social engineering attacks.

Source: IDC's *Government Survey,* conducted for Akamai, August/September 2023 (N = 100)

In response to new security and privacy imperatives, European legislators are actively shaping the regulatory framework, requiring governments to adapt

Key Regulations Influencing IT and Cybersecurity Strategy



Founded upon the General Data Protection Regulation, the European regulatory framework includes an increasing number of provisions that promote the secure, transparent, resilient, responsible, and ethical use of data and technology.

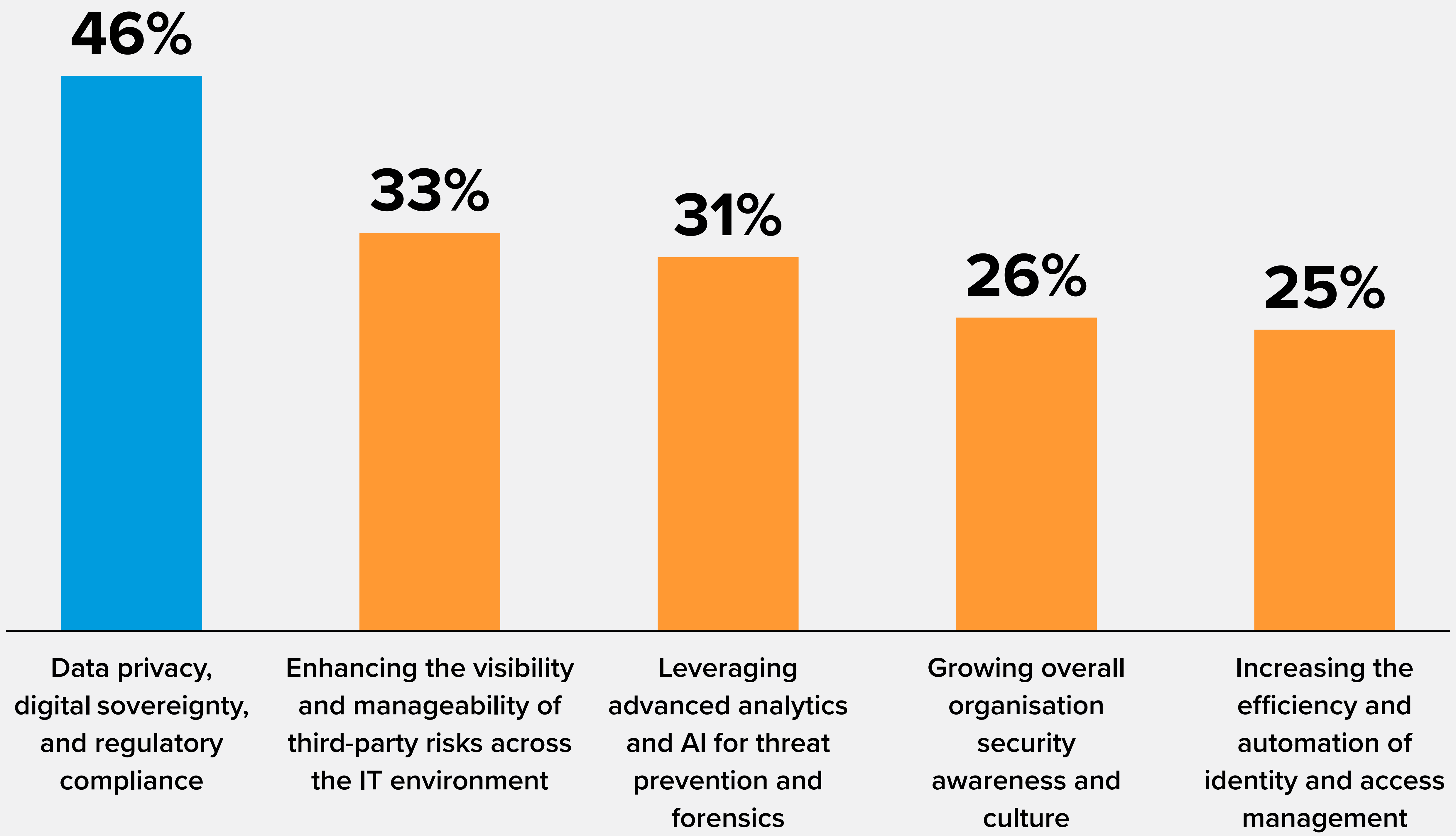
These laws, policies, and procedures define the mandates, guidelines, and best practices necessary to ensure that next-generation public services — whether delivered directly by governments or in partnership with the private sector — are trusted by citizens and civil servants.

Public organisations need to adapt to these regulations and rethink their internal processes.

Source: IDC's *Government Survey,* conducted for Akamai, August/September 2023 (N = 100)

Data security and compliance form the cornerstone of secure and trusted operations

Top 5 IT Security Operational Priorities



Adherence to complex regulations, including those around data privacy, is pivotal to building public trust, preserving national/local security, and mitigating data breach and noncompliance risks.

These are the critical outcomes to regulatory compliance:

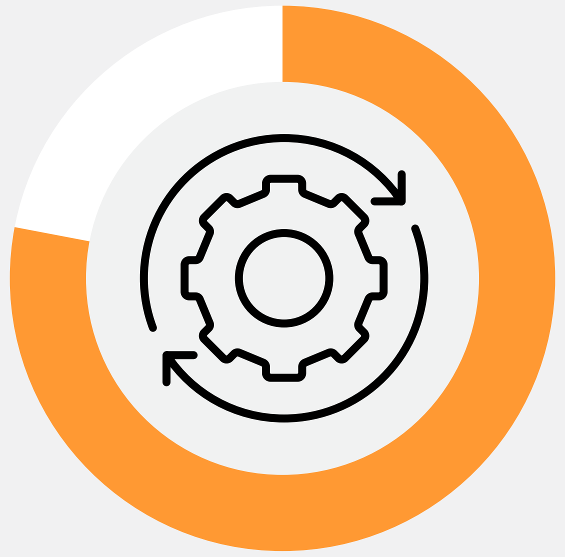
- Enhanced data protection
- Digital sovereignty assurance
- Critical infrastructure protection
- Efficient service delivery

Source: IDC's *Government Survey,* conducted for Akamai, August/September 2023 (N = 100)

Transforming Legacy Security Systems

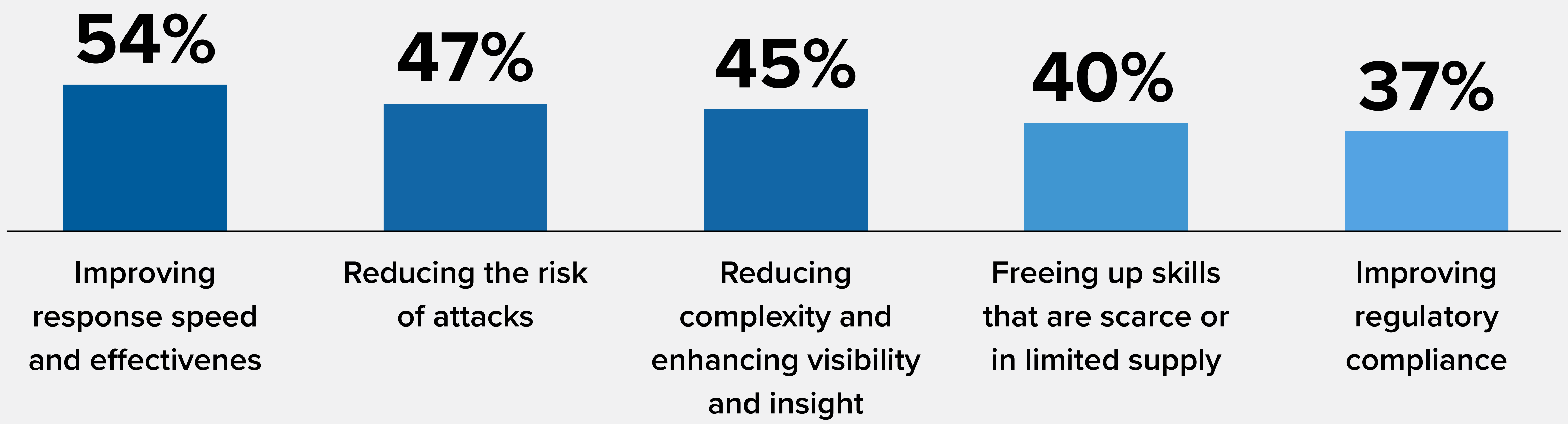
Timeline for Transforming Legacy Security Systems

78%



Plan to implement within **48 months**

Expected Benefits of Modernising Legacy Security Systems



The Complexity and Challenges Associated with Modernising Legacy Infrastructure

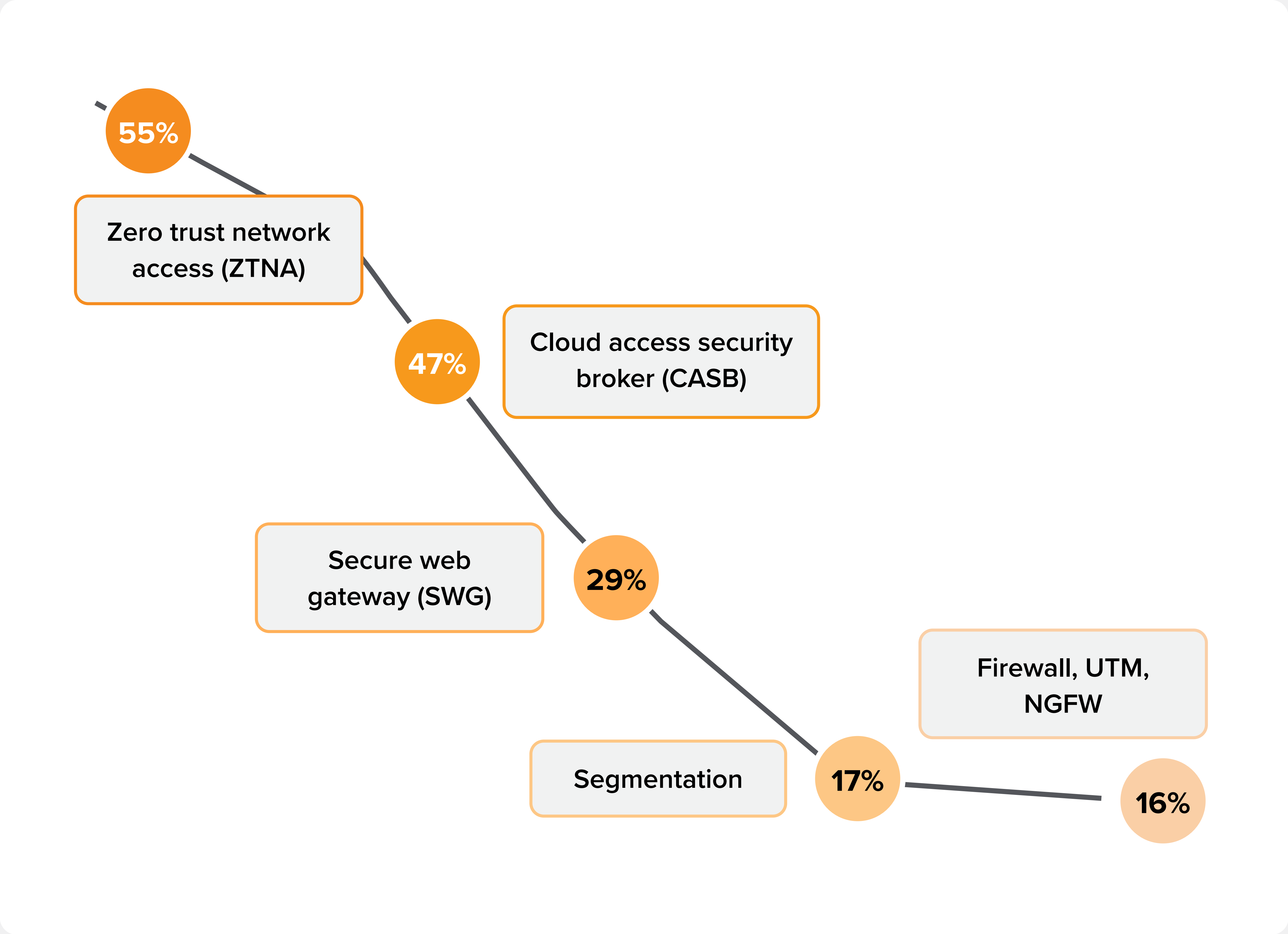
- **Complexity of Legacy Systems:** Legacy security systems often consist of a complex patchwork of technologies that may not adequately address modern threats. Their outdated nature can leave critical assets vulnerable.
- **Budget and Resource Constraints:** Resource limitations include budget constraints and the need for skilled personnel to oversee modernisation efforts.
- **Lack of Security Maturity:** Security needs to be elevated to meet modern standards, and legacy systems need transforming, which requires additional time and effort.
- **Data Sensitivity:** Protecting sensitive data is critical. Ensuring a secure transition to modern security systems is imperative to safeguarding this information.
- **Security Fragmentation:** Legacy security systems often operate in isolation, creating management, coordination, and overall security effectiveness challenges.

78% plan to modernise legacy security systems within 48 months, recognising this essential step in achieving a robust and resilient security framework to protect critical assets, data, and users.

Source: IDC's *Government Survey,* conducted for Akamai, August/September 2023 (N = 100)

Holistic Approach to Network Security: Driving Efficiency and Zero Trust Assurance

Network Security Priorities



These technologies will play a pivotal role in **shaping the future of public sector cybersecurity** and collectively provide a comprehensive security framework that minimises attack surfaces, reduces risks, and protects critical assets.

Data Protection: Robust security measures safeguard sensitive data, even in cloud environments, ensuring compliance with regulations.

Efficiency: Micro-segmentation and ZTNA enable efficient network access control, reducing the risk of lateral cyberthreat movement.

Improved User Experience: ZTNA ensures secure access to applications from anywhere, enhancing user productivity.

Business Continuity: These technologies are part of a holistic approach to safeguarding government operations and services, ensuring continuity regardless of cyberthreats.

Enhanced Trust: The implementation of zero trust technologies also enhances public trust in government institutions. Trust and reputation are invaluable assets in the public sector, contributing to citizen confidence and support.

The adoption of zero trust technologies significantly enhances security posture. It enables efficient and secure access to resources and protects sensitive data, ensuring the continuity of government services and increasing overall resilience to cyberthreats.

Source: IDC's *Government Survey,* conducted for Akamai, August/September 2023 (N = 100)

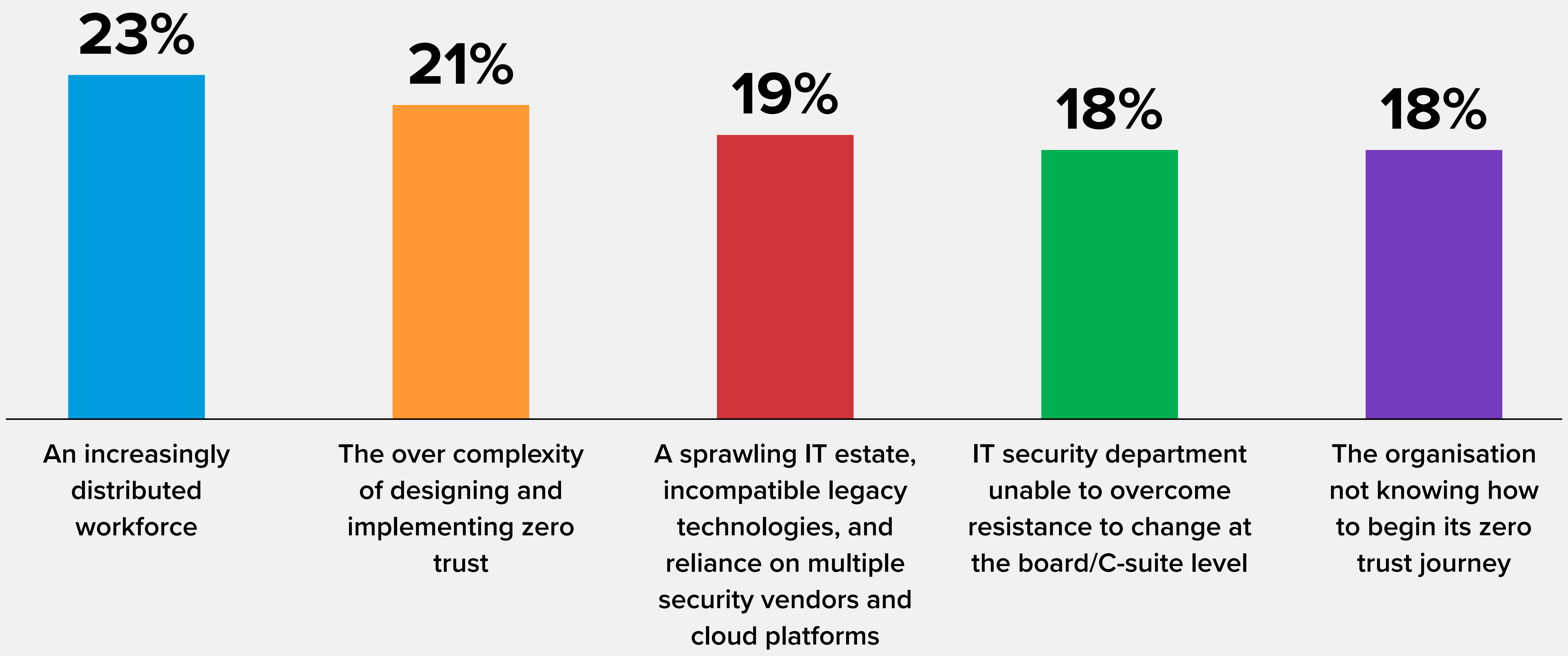
Zero Trust for Secure and Resilient Government Operations

The adoption of zero trust models is a **strategic priority for 91%** of public sector organisations. The benefits are clear: **enhanced security, reduced risk** of insider threats, and **improved resilience** against cyberattacks.

The adoption of zero trust in the public sector has a strong impact. Zero trust **safeguards citizen data** and critical government systems against new and emerging cybersecurity risks.

By implementing zero trust, government organisations can ensure the **highest level of security, strengthen national/local security, and protect the sensitive data entrusted to them by citizens**.

Challenges to Zero Trust Adoption



While challenges persist, none is perceived as an unmoveable barrier to transformation, reflecting the public sector's commitment to building a strong cybersecurity posture. **Collaboration with the right partners** will enable public sector organisations to **address zero trust complexity** seamlessly, ensuring **optimal protection for critical digital assets**.

Source: IDC's *Government Survey,* conducted for Akamai, August/September 2023 (N = 100)

Addressing Citizen Experience & Trust, Cyber Resilience, and Civil Servant Experience Priorities Through Security

Technologies	Business Outcomes
API security	○ Secure interactions with external systems ○ Increased data integrity through APIs ○ Integration without disruption
ZTNA	○ Secure access anywhere, anytime ○ Reduced risk of unauthorised access ○ Better user experience
Micro-segmentation	○ Granular security controls ○ Reduced lateral threat movement ○ Streamlined compliance
Multifactor authentication	○ Strengthened security around citizen data ○ Improved access control ○ Enhanced trust in digital interactions

Application Security

Top concern — data breaches and data leakage: 49%

Top challenge — limited visibility into applications: 47%

API security tools will guarantee the secure exchange of data between systems, ensuring integrity and confidentiality. API security can enable resilient interconnected systems, fortify the overall cybersecurity posture, and deliver efficient and trusted services.

By leveraging zero trust technologies — including MFA, ZTNA, micro-segmentation, and API security — public sector organisations can improve security posture and build trust in digital interactions.

The approach prioritises seamless citizen experiences across secure government services. Process automation will not only address the skills gap but also ease resistance to change by simplifying security processes, reducing manual efforts, and lightening the workload on security teams, thus creating a more agile and responsive security posture.

Essential Guidance

Zero trust is a top priority; it will support organisations' journeys.

Zero trust has become the gold standard for modern cybersecurity, playing a crucial role in ensuring resilience in public services operations.

Acknowledging the challenges associated with its implementation, public services should **seek support to integrate zero trust principles** and streamline technology deployments. This strategic shift will be key to more efficient, agile, and resilient security operations.

Cybersecurity investments need to align with government priorities.

Not all governments are equal. National government ministries are organised around large departments that work in silos, but they increasingly need to share data and must **tackle risks arising from internal data exchange**.

Local governments have limited resources and struggle to monitor vulnerabilities across the growing range of citizen services they need to provide online. They **should invest in solutions that can improve risk visibility**.

Innovation is falling behind due to a lack of skills and a reluctance to change.

In general, organisations struggle with a lack of skills — which prevents them from innovating — and with a mindset resistant to new ways of working.

They should **select strategic cybersecurity partners** able to deliver solutions that are easy to use, interoperable with existing systems, and can be incrementally implemented to reduce the resistance that arises when big rip-and-replace projects are pushed through.

Trust and citizen experience go hand in hand.

Public services should **articulate the value of cybersecurity** in terms of internal risk reduction — technical, organisational, and compliance — and, more importantly, **improved public confidence** in digital government services and the handling of sensitive citizen data.

This will enable better alignment of cybersecurity efforts with broader public service objectives.

Message from Sponsor

Akamai protects your citizen experience, workforce, systems, and data by helping to embed security into everything you create—anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture to enable zero trust, stop ransomware, secure apps and APIs, and defend against DDoS attacks, giving you the confidence to continually innovate, expand, and transform.

Learn more about Akamai's cloud computing, security, and content delivery solutions at **www.akamai.com.**

Akamai

Appendix

Methodology

Survey Purpose

Senior government leaders in EMEA and beyond are embracing technological innovation to shape the next generation of public services. Accelerated digital transformation has heightened challenges around data protection and operational security. This survey investigates how senior civil servants are investing in cybersecurity to enhance resilience and enable digital transformation.

Sample Qualification

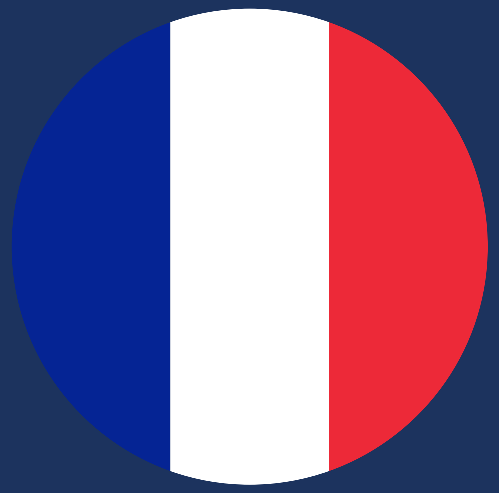
- Conducted in four countries
- Organisations with 100+ employees
- National, regional, and local governments
- Respondents: with a role in IT products and services spending, including IT security

Survey Design

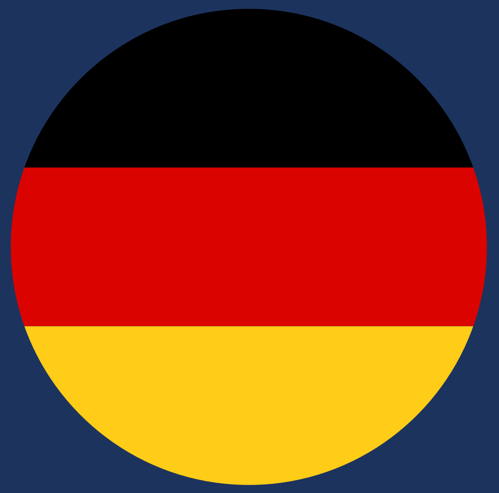
CATI, conducted in August and September 2023

Survey Topics

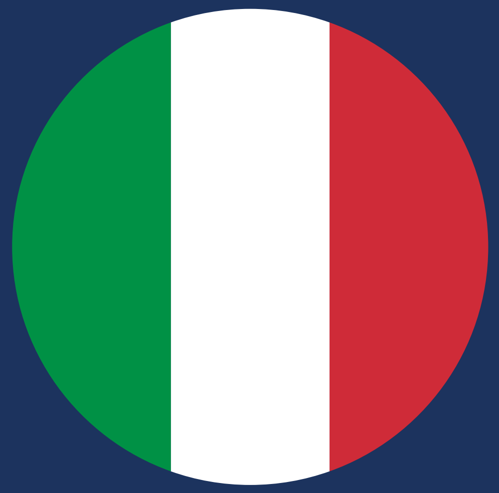
- Drivers of and challenges to government organisations' digital transformation
- Cybersecurity drivers, challenges, and investments



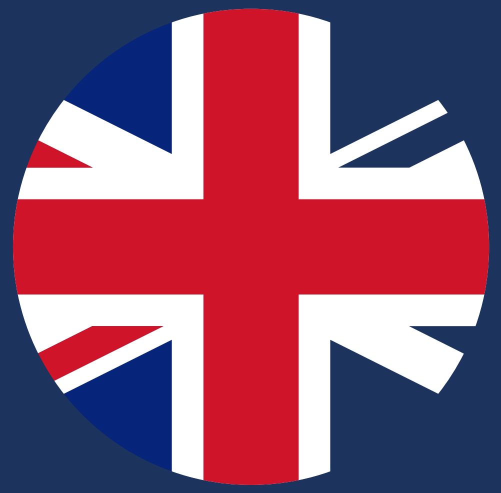
N = 22



N = 27



N = 22



N = 29

Sample — Company Size, Subsector, Title, and Decision Role

35% 100–499 employees

65% 500 or more employees

80% National government

20% Regional and local government

29% C level

71% VP/Director

15% Primary decision maker

41% Part of decision team

44% Knowledgeable influencer

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets.

With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG, Inc.), the world's leading tech media, data and marketing services company.

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.

IDC UK
5th Floor, Ealing Cross, 85 Uxbridge Road, London, W5 5TH, United Kingdom
T 44.208.987.7100

@idc   @idc   idc.com

© 2024 IDC Research, Inc. IDC materials are licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.